Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (original) A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge.

2. (original) The system as claimed in claim 1, wherein said token device receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

3. (original) The system as claimed in claim 1, further

comprising a third party server, wherein a response to said integrity challenge is sent to said third party server.

4. (original) The system as claimed in claim 3, wherein said monitoring component sends a detailed integrity response to a third party server if requested to do so in said integrity challenge.

5. (previously presented) The system as claimed in claim 3, wherein said monitoring component reports a detailed integrity response to said token device and said token device sends said integrity response to said third party server if it requires the third party server to help interpret said detailed integrity response.

6. (previously presented) The system as claimed in claim 3, in which a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

7. (previously presented) The system as claimed in claim 6, wherein a third party server sends a simplified integrity response to said token device.

8. (previously presented) The system as claimed in claim 7,

operating to add a digital signature data to said simplified integrity response, said digital signature authenticating said third party server to said token device.

9. (previously presented) The system as claimed in claim 1, wherein said monitoring component sends a detailed integrity response to a third party server.

10. (previously presented) The system as claimed in claim 1, in which said token device is requested to take an action.

11. (previously presented) The system as claimed in claim 1 in which said token device requests to take an action.

12. (previously presented) The system as claimed in claim 1 in which said token device sends image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform displays said image data.

13. (original) The system as claimed in claim 1, wherein said monitoring component is capable of establishing an identity of itself.

14. (original) The system as claimed in claim 1, further comprising an interface means for interfacing between said monitoring component and said token device.

15. (previously presented) The system as claimed in claim 1, wherein said system of computing apparatus is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

16. (original) The system as claimed in claim 1, wherein a said specific action comprises authorising said computing platform to undertake a transaction on behalf of a user of said system.

17. (original) A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device beingphysically distinct and separable from said computing platform and said monitoring component,

wherein said token device sends an integrity challenge to said monitoring component;

said monitoring component generates a response to said integrity challenge;

if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform; and

said computer platform displays said verification data on a visual display screen.

18. (original) A computing entity comprising:

a computing platform having a first data processor and first data storage means;

a monitoring component having a second data processor and second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform, said monitoring component being capable of establishing an identity of itself.

interface means for communicating with a token device, said interface means communicating with said monitoring component,

wherein said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

19. (original) The computing entity as claimed in claim 18,

wherein on communication between said token device and said interface means, said monitoring component is activated to perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

20. (original) The computing entity as claimed in claim 18, wherein said interface means is resident substantially wholly within said monitoring component.

21. (currently amended) The computing entity as claimed in claim 18, wherein said interface means ~~comprises~~ is comprised by said computer platform.

22. (original) The computing entity as claimed in claim 18, wherein said interface means comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0.

23. (original) The computing entity as claimed in claim 18, wherein said monitoring component comprises a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means.

24. (original) The computing entity as claimed in claim 18,

wherein said interface means is configured to send and receive data according to a pro-active protocol.

25. (original) A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform comprising a first data processor and a first memory means, and a monitoring component comprising a second data processor and a second memory means, said method comprising the steps of:

receiving an interrogation request signal via an interface of said computing entity;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and

said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation.

26. (original) A method as claimed in claim 25, in which said monitoring operation comprises the steps of:

said monitoring component carrying out one or a plurality of data checks on components of said computing platform; and

said monitoring component being able to report a set of certified reference data together with said data checks.

27. (previously presented) The method as claimed in claim 26, wherein said certified reference data includes a set of metrics to be expected when measuring particular components of said computing platform, and includes digital signature data identifying an entity that certifies said reference data.

28. (original) The method as claimed in claim 25, wherein said step of reporting verification of said monitoring operation comprises sending a confirmation signal to a token device said confirmation signal describing a result of said monitoring operation.

29. (original) The method as claimed in claim 25, wherein said result message is transmitted by said interface to a token device external of said computing entity.

30. (original) The method as claimed in claim 25, comprising the step of reporting a result of said monitoring operation by generating a visual display of confirmation data.

31. (original) The method as claimed in claim 25, further comprising the step of adding a digital signature data to said result message, said digital signature data identifying said monitoring component; and

transmitting said result message and said digital signature

data from said interface.

32. (original) A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component, said method comprising the steps of:

an application requesting access to a functionality from a token device;

in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component;

in response to said request for verification, said monitoring component reporting a result message to said token device, said result message describing a result of a monitoring operation;

by receipt of a satisfactory said result message, said token device offers said functionality to said application.

33. (original) The method as claimed in claim 32, wherein said monitoring component sends a detailed integrity response to a third party server if requested in an integrity challenge by said token device.

34. (original) The method as claimed in claim 32, wherein said monitoring component reports a detailed integrity response to

said token device, and said token device sends said integrity response to a third party server if it requires the third party server to help interpret said detailed integrity response.

35. (currently amended) The method as claimed in claim ~~32~~ 34, wherein a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

36. (original) The method as claimed in claim 32, wherein a third party server sends a simplified integrity response to said token device.

37. (original) The method as claimed in claim 32, further comprising the steps of:

adding a digital signature data to a simplified integrity response, said digital signature data authenticating a third party server to said token device.

38. (original) A method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means, and a monitoring component comprising a second processor and second memory means, by means of a token device, said token device comprising a third data processor and a third memory

means, said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform;

said token device receiving a poll signal from said computer platform;

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component; and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device.

39. - 40. (canceled)

41. (previously presented) The token device as claimed in claim 44, said device being configured to be responsive to a poll signal operating in accordance with PC/SC specification 1.0, said token device being capable of initiating a command to be handled by a software stack on the computer entity, in response to said poll signal according to said poll signal according to a proactive protocol.

42. (original) A method of verifying a status of a computing entity, by means of a token device provided external of said

computing entity, said method comprising the steps of:

said token device receiving a poll signal;

said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity; and

said token device receiving a result message, said result message describing the result of said verification.

43. (original) A method by which a token device can obtain verification of a state of a computing platform by using a monitoring component,

said monitoring component being capable of performing at least one data check on said computer platform, and establishing an identity of itself, and establishing a report of said at least one data check; and

wherein said token device has data processing capability and behaves in an expected manner;

said token device being physically separable from said computing platform and said monitoring component, said token device having cryptographic data processing capability

wherein, said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computing platform.

44. (original) A token device comprising a data processor and a memory device, said token device configured to perform at least one data processing or signaling function:

wherein said token device operates to:

receive an integrity check data from an external source;

if said integrity check data supplied to said token device is satisfactory, then said token device allows a said function; and

if said integrity check data received by said token device is unsatisfactory, then said token device denies said function.

45. (previously presented) A system as claimed in claim 1, wherein said token device is a smart card.

46. (previously presented) A system as claimed in claim 18, wherein said token device is a smart card.

47. (previously presented) A token device as claimed in claim 44 in the form of a smart card.

48. (previously presented) A computing system comprising:

a computing apparatus having a first data processor and a first memory;

a monitoring component having a second data processor and a second memory, wherein said monitoring component is configured to perform a plurality of data checks on said computing apparatus; and

a portable user token being physically distinct and separable from said computing apparatus and said monitoring component,

wherein in one mode of operation, said portable user token operates to make an integrity challenge to said monitoring component and said user computing device will not undertake specific actions of which it is capable unless a satisfactory response to said integrity challenge is provided.

49. (previously presented) The system as claimed in claim 48, wherein said portable user token receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

50. (previously presented) The system as claimed in claim 48, in which said portable user token is requested to take an action.

51. (previously presented) The system as claimed in claim 48 in which said portable user token requests to take an action.

52. (previously presented) The system as claimed in claim 48, wherein said monitoring component is capable of establishing an identity of itself.

53. (previously presented) The system as claimed in claim 48, further comprising token interface for interfacing between said monitoring component and said portable user token.

54. (previously presented) The system as claimed in claim 48, wherein said computing system is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer apparatus.

55. (previously presented) The system as claimed in claim 48, wherein the monitoring component is mounted on a common assembly with the first processor.

56. (previously presented) The system as claimed in claim 48, wherein one or more of said data checks comprise a check of the integrity of the basic input/output software for one or more components of the computing apparatus.

57. (previously presented) The system as claimed in claim 48, wherein the portable user token is a smart card.

58. (previously presented) The system as claimed in claim 53, wherein the portable user token is a smart card, and the token interface comprises a smart card reader.

59. (previously presented) A computing entity comprising:

a computing platform having a first data processor and a first memory;

a monitoring component having a second data processor and a second memory, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform,

a communications interface for communicating with a portable user token, said communications interface having a communication path to the monitoring component,

wherein said computing entity is configured such that said monitoring component is adapted to report said data checks to a portable user token connected to the communications interface, said data checks containing data describing a status of said computing platform.

60. (previously presented) The computing entity as claimed in claim 59, wherein on communication between said portable user token and the communications interface, said monitoring component is activated to perform a monitoring operation on said

computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

61. (previously presented) The computing entity as claimed in claim 59, wherein the communications interface is a smart card reader.